UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/405,031	09/24/1999	DOUGLAS R. COFFLAND	IL-10360	9034

7590 01/13/2005

LLOYD E DAKIN JR
ASSISTANT LABORATORY COUNSEL
LAWRENCE LIVERMORE NATIONAL LABORATORY
P O BOX 808-L-703
LIVERMORE, CA 94551

EXAMINER	
BETIT, JACOB F	
ART UNIT	**PAPER NUMBER**
2164	

DATE MAILED: 01/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application N .	Applicant(s)	
	09/405,031	COFFLAND, DOUGLAS R.D	
	Examiner	Art Unit	
	Jacob F. Betit	2164	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 September 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

SAM RIMELL
PRIMARY EXAMINER

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Remarks

1. In response to communications filed on 29-September-2004, claims 1, 10, 17, and 24 are amended per applicant's request. Claims 1-30 are presently pending in the application.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-5, 9-14, 17-21, and 24-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Noll et al. (U.S. patent No. 5,732,138) in view of Koopman, Jr. (U.S. patent No. 5,757,923.

As to claim 1, Noll et al. teaches a system for multimedia encryption comprising:

acquisition means for acquiring a media signal, that has the capacity of containing random noise that is completely unpredictable from one moment to the next (see column 4, line 46 through column 5, line 17, where chaotic systems are unpredictable "from one moment to the next" when the difference between moments is not a small amount of time);

data acquisition means to receive and select a set of data from the data stream (see figure 1, steps 100, and 105); and

hashing means coupled to the data acquisition means to receive and hash the set of data into a keyword (see column 4, lines 20-23, where "keyword" is read on "seed").

Noll et al. does not teach data compression means coupled to the acquisition means to receive and compress the media signal containing random noise that is completely unpredictable from one moment to the next into a compressed data stream; and data acquisition means coupled to the data compression means to receive and select a set of data from the compressed data stream.

Koopman, Jr. teaches generating secret identification numbers from a random digital data stream (see abstract), in which he teaches data compression means coupled to the acquisition means to receive and compress the media signal containing random noise that is completely unpredictable from one moment to the next into a compressed data stream; and data acquisition means coupled to the data compression means to receive and select a set of data from the compressed data stream (see column 7, lines 1-25).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Noll et al. by the teachings of Koopman, Jr. because data compression means coupled to the acquisition means to receive and compress the media signal containing random noise that is completely unpredictable from one moment to the next into a compressed data stream; and data acquisition means coupled to the data compression means to receive and select a set of data from the compressed data stream would improve the entropy per bit which would better approximate true randomness (see Koopman, Jr., column 7, lines 1-15).

As to claim 2, Noll et al. as modified, teaches wherein the set of data is one frame of data within the compressed data stream (see Noll et al., column 4, lines 61-62).

As to claim 3, Noll et al. as modified, teaches wherein the set of data crosses over several frame boundaries within the compressed data stream (see Noll et al., column 4, lines 60-61).

As to claim 9, Noll et al. as modified, teaches further comprising:

a pseudo-random number generator coupled to receive and process the keyword in to a set of keywords (see Noll et al., column 4, lines 23-26).

As to claim 10, Noll et al. teaches a method for multimedia encryption, comprising the steps of:

acquiring a media signal that has the capacity of containing random noise that is completely unpredictable from one moment to the next (see column 4, line 46 through column 5, line 17, where chaotic systems are unpredictable "from one moment to the next" when the difference between moments is not a small amount of time);

selecting a set of data from the media signal (see figure 1, steps 100, and 105); and

hashing the set of data into a keyword (see column 4, lines 20-23, where "keyword" is read on "seed").

Noll et al. does not teach compressing the media signal, the media signal having

the capacity of containing random noise that is completely unpredictable from one moment to the next; selecting a set of data from the compressed media signal.

Koopman, Jr. teaches compressing the media signal, the media signal having the capacity of containing random noise that is completely unpredictable from one moment to the next; selecting a set of data from the compressed media signal (see column 7, lines 1-25).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Noll et al. by the teachings of Koopman, Jr. because compressing the media signal, the media signal having the capacity of containing random noise that is completely unpredictable from one moment to the next; selecting a set of data from the compressed media signal would better approximate true randomness (see Koopman, Jr., column 7, lines 1-15).

As to claim 17, Noll et al. teaches a system for multimedia encryption, comprising:

acquisition means for acquiring a media signal, the media signal having the capacity of containing random noise that is completely unpredictable from one moment to the next (see column 4, line 46 through column 5, line 17, where chaotic systems are unpredictable "from one moment to the next" when the difference between moments is not a small amount of time);

selection means for selecting a set of data from the data stream (see figure 1, steps 100, and 105); and

hashing means coupled to said selection means for hashing the set of data into a keyword (see column 7, lines 1-25).

Noll et al. does not teach data compression means coupled to said acquisition means to receive and compress said media signal containing random noise that is completely unpredictable from one moment to the next into a compressed data stream; and selection means coupled to said data compression means for selecting a set of data from the compressed data stream.

Koopman, Jr. teaches data compression means coupled to said acquisition means to receive and compress said media signal containing random noise that is completely unpredictable from one moment to the next into a compressed data stream; and selection means coupled to said data compression means for selecting a set of data from the compressed data stream (see column 7, lines 1-25).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Noll et al. by the teachings of Koopman, Jr. because data compression means coupled to said acquisition means to receive and compress said media signal containing random noise that is completely unpredictable from one moment to the next into a compressed data stream; and selection means coupled to said data compression means for selecting a set of data from the compressed data stream would better approximate true randomness (see Koopman, Jr., column 7, lines 1-15).

As to claim 24, Noll et al. teaches a computer-useable medium embodying computer program code for multimedia encryption by executing the steps of:

acquiring a media signal, said media signal having the capacity of containing random noise that is completely unpredictable from one moment to the next (see column 4, line 46 through column 5, line 17, where chaotic systems are unpredictable "from one moment to the next" when the difference between moments is not a small amount of time);

selecting a set of data from the media signal (see figure 1, steps 100, and 105); and

hashing the set of data into a keyword (see column 4, lines 20-23, where "keyword" is read on "seed").

Noll et al. does not teach compressing said media signal, the media signal having the capacity of containing random noise that is completely unpredictable from one moment to the next; selecting a set of data from the compressed media signal.

Koopman, Jr. teaches compressing said media signal, the media signal having the capacity of containing random noise that is completely unpredictable from one moment to the next; selecting a set of data from the compressed media signal (see column 7, lines 1-25).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Noll et al. by the teachings of Koopman, Jr. because compressing said media signal, the media signal having the capacity of containing random noise that is completely unpredictable from one moment to the next; selecting a set of data from the compressed media signal would better approximate true randomness (see Koopman, Jr., column 7, lines 1-15).

As to claims 4, 13, 20, and 27 Noll et al. as modified, teaches wherein:

the compressed data stream includes compression transform coefficients; and the set of data includes a set of compression transform coefficients (see Koopman, Jr., column 7, lines 25-59).

As to claims 5, 14, 21, and 28 Noll et al. as modified, teaches wherein:

the compressed data stream includes data frames of varying length (see Koopman, Jr., column 7, lines 25-59); and

the set of data includes a set of data frames (see Noll et al., column 4, lines 56-67).

As to claims 11, 18, and 25 Noll et al. as modified, teaches wherein:

the compressed media signal includes data frames (see Koopman, Jr., column 7, lines 16-59); and

the selecting step includes the step of selecting one frame of data (see Noll et al., column 4, lines 56-67).

As to claims 12, 19, and 26 Noll et al. as modified, teaches wherein:

the compressed media signal includes data frames and data frame boundaries (see Koopman, Jr., column 7, lines 16-59); and

the selecting step includes the step of selecting a set of data which crosses over several data frame boundaries (see Noll et al., column 4, lines 56-67).

4. Claims 6, 8, 15, 22, and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Noll et al. (U.S. patent No. 5,732,138) in view of Koopman, Jr. (U.S. patent No. 5,757,923 as applied to claims 1-5, 9-14, 17-21, and 24-28 above, and further in view of Owashi et al. (U.S. patent No. 6,363,210 B1).

As to claims 6, 15, 22, and 29 Noll et al. as modified, still does not teach wherein:

the compressed data stream includes predictive data frames; and

the set of data includes a predictive data frame.

Owashi et al. teaches encrypting communication signals (see abstract), in which he teaches wherein: the compressed data stream includes predictive data frames; and the set of data includes a predictive data frame (see column 9, lines 5-13).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Noll et al. as modified, by the teachings of Owashi et al. because wherein: the compressed data stream includes predictive data frames; and the set of data includes a predictive data frame would be the most obvious form of compression for video media (see Owashi et al., column 14, lines 29-31).

As to claim 8, Noll et al. as modified, still does not teach wherein the data compression module compresses the media signal into one from a group consisting of: MJPEG, MPEG1, MPEG2, or MPEG4, H.261, H.320, and H.323 formats.

Owashi et al. teaches wherein the data compression module compresses the media signal into one from a group consisting of: MJPEG, MPEG1, MPEG2, or MPEG4, H.261, H.320, and H.323 formats (see column 9, lines 5-13).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Noll et al. as modified, by the teachings of Owashi et al. because wherein the data compression module compresses the media signal into one from a group consisting of: MJPEG, MPEG1, MPEG2, or MPEG4, H.261, H.320, and H.323 formats would be the most obvious form of compression for video media (see Owashi et al., column 14, lines 29-31).

5. Claims 7, 16, 23, and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Noll et al. (U.S. patent No. 5,732,138) in view of Koopman, Jr. (U.S. patent No. 5,757,923) as applied to claims 1-5, 9-14, 17-21, and 24-28 above, and further in view of Borza et al. (U.S. patent No. 6,215,874 B1).

As to claim 7, Noll et al. as modified, wherein the data compression module compresses the quantized media signal into a compressed data stream (see Koopman, Jr., column 7, lines 1-59).

Noll et al. as modified, does not teach wherein the media signal includes a noise signal amplitude; further comprising, an analog to digital converter, having a quantization step size smaller than the noise signal amplitude, coupled to receive and quantize the media signal.

Borza et al. teaches wherein the media signal includes a noise signal amplitude (see column 5, lines 4-16); further comprising, an analog to digital converter, having a quantization step size smaller than the noise signal amplitude, coupled to receive and quantize the media signal (see column 6, lines 21-33).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Noll et al. by the teachings of Borza et al. because wherein the media signal includes a noise signal amplitude; further comprising, an analog to digital converter, having a quantization step size smaller than the noise signal amplitude, coupled to receive and quantize the media signal would produce a random number to be used as a deed in a pseudo random number generator that would be more random than if just a regular image was used by itself (Borza et al., column 10, lines 4-12).

As to claims 16, 23, and 30 Noll et al. as modified, teaches

wherein the compressing step includes the step of compressing the quantized media signal (see Koopman, Jr., column 7, lines 1-59).

Noll et al. does not teach wherein the media signal includes a noise signal amplitude; further comprising the step of quantizing the media signal with a quantization step size smaller than the noise signal amplitude.

Borza et al. teaches wherein the media signal includes a noise signal amplitude (see Borza et al., column 5, lines 4-16); further comprising the step of quantizing the media signal with a quantization step size smaller than the noise signal amplitude (see Borza et al., column 6, lines 21-33).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Noll et al. by the teachings of Borza et al. because wherein the media signal includes a noise signal amplitude; further comprising the step of quantizing the media signal with a quantization step size smaller than the noise signal amplitude would produce a random number to be used as a deed in a pseudo random number generator that would be more random than if just a regular image was used by itself (Borza et al., column 10, lines 4-12).

Response to Arguments

6. Applicant's arguments filed 29-September-2004 have been fully considered but they are not persuasive.

In response to the applicant's arguments that "Since the Noll et al reference is limited to a "chaotic source" the Noll et al reference system can not be modified to include Applicant's claim elements, 'acquisition source for acquiring a media signal that has the capacity of containing random noise that is completely unpredictable from one moment to the next into a compressed data stream'", the arguments have been fully considered but are not deemed persuasive because a "chaotic" noise seems to fit in the applicants definition of a "random" noise. The applicant defines a random noise as completely unpredictable from one moment of time to the next. A chaotic noise would be completely unpredictable from "one moment of time to the next" for all instances except when the difference between the moments of time is "small" (Noll et al., column 2, lines 5-19).

In response to the applicant's arguments that there is no motivation to combine the Noll et al. reference with the Koopman, Jr. reference or the Borza et al. reference the arguments have been fully considered but are not deemed persuasive because there is motivation to combine both of these references with the Noll et al. reference found in the office action dated 29-July-2004. The motivation to combine the Noll et al. reference with the Koopman, Jr. reference is found on page 4, lines 16-21; on page 7, lines 11-15; on page 9, lines 1-5, and on page 10, lines 11-15 of that office action. The motivation to combine the Noll et al. reference as previously modified by the Koopman, Jr. reference and further modified by the Borza et al. reference is found on page 5, lines 15-21; on page 8, lines 3-7; on page 9, on lines 14-18; and on page 11, lines 3-7 of that office action. Furthermore motivation to combine all references used in this office action can be found in this office action as part of the 35 U.S.C. 103(a) rejections found above as required by the MPEP.

In response to the applicants arguments that there is no motivation to combine the Noll et al. reference with the Koopman, Jr. reference, the Borza et al. reference, and the Owashi et al. reference the arguments have been fully considered, but are not deemed persuasive because there is motivation to combine these references found in the office action dated 29-July-2004. The motivation to combine the Noll et al. reference with the Koopman, Jr. reference and the Borza et al. reference was pointed out in the arguments above. The motivation to combine Noll et al. reference as previously modified by Koopman, Jr. reference and Borza et al. reference can be found on page 13, lines 11-15

and on page 14, lines 8-13. Furthermore motivation to combine all references used in this office action can be found in this office action as part of the 35 U.S.C. 103(a) rejections found above as required by the MPEP.

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jacob F. Betit whose telephone number is (703) 305-3735. The examiner can normally be reached on Monday through Friday 9 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Dov Popovici can be reached on (703) 305-3830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

jfb

4 Jan 2005

SAM RIMELL
PRIMARY EXAMINER